Interference & updated search

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	central.clm. and client.clm. and transmit$4.clm. and remote.clm. and "partial response".clm. and display$3.clm. and nonce.clm. and authoriz44.clm. and sign$4.clm. and digital$5.clm. and access$2. clm. and value.clm.	USPAT	OR	OFF	2006/07/10 16:10
L2	0	central.clm. and client.clm. and transmit$4.clm. and remote.clm. and "partial response".clm. and display$3.clm. and nonce.clm. and authoriz44.clm. and sign$4.clm. and digital$5.clm. and access$2. clm. and value.clm.	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:10
L3	0	central.clm. and client.clm. and transmit$4.clm. and remote.clm. and "partial response".clm. and display$3.clm. and nonce.clm. and authoriz$4.clm. and sign$4.clm. and digital$5.clm. and access$2. clm. and value.clm.	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:11
L4	0	client.clm. and transmit$4.clm. and remote.clm. and "partial response".clm. and display$3.clm. and nonce.clm. and authoriz$4. clm. and sign$4.clm. and digital$5.clm. and access$2.clm. and value.clm.	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:11
L5	0	client and transmit$4 and remote and "partial response" and display$3 and nonce and authoriz and sign$4 and digital$5 and access$2 and value	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:13
L6	0	client and transmit$4 and remote and display$3 and nonce and authoriz and sign$4 and digital$5 and access$2 and value	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:13
L7	195	client and transmit$4 and remote and display$3 and nonce and authoriz$3 and sign$4 and digital$5 and access$2 and value	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:13
L8	7	client and transmit$4 and remote and "partial response" and display$3 and nonce and authoriz$4 and sign$4 and digital$5 and access$2 and value	US-PGPUB; USPAT	OR	OFF	2006/07/10 16:14

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

client and transmit$4 and remote and "partial response" and d

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **client** and **transmit$4** and **remote** and **partial response** and **display$3** and **nonce** and **authoriz$4** and **sign$4** and **digital$5** and **access$2** and **value**

Founc
167 o
178,88(

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 167 Result page: **1** 2 3 4 5 6 7 8 9 next

Relevance scale

1 Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks
Haidong Xia, José Carlos Brustoloni
May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**
Publisher: ACM Press
Full text available: pdf(770.11 KB) Additional Information: full citation, abstract, references, index terms

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

Keywords: HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

2 Remote operations across a network of small computers
Brent Nordin, Ian A. Macleod, T. Patrick Martin
December 1986 **Proceedings of the 1986 ACM SIGSMALL/PC symposium on Small systems**
Publisher: ACM Press
Full text available: pdf(465.42 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper discusses the design of a Remote Operation Call (ROC) mechanism. ROCs are a generalisation of the remote procedure call concept. They provide for a wider variety of remote calls, such as asynchronous, directed and multicast calls. An implementation of ROCs on a network of personal computers is also described.

3 Session 2: secure Web services: Validating a Web service security abstraction by typing
Andrew D. Gordon, Riccardo Pucella
November 2002 **Proceedings of the 2002 ACM workshop on XML security**
Publisher: ACM Press

Full text available: pdf(210.31 KB) Additional Information: full citation, abstract, references, citings, index terms

An XML web service is, to a first approximation, an RPC service in which requests and responses are encoded in XML as SOAP envelopes, and transported over HTTP. We consider the problem of authenticating requests and responses at the SOAP-level, rather than relying on transport-level security. We propose a security abstraction, inspired by earlier work on secure RPC, in which the methods exported by a web service are annotated with one of three security levels: none, authenticated, or both authen ...

Keywords: Web services, authentication, remote procedure call, type systems

4 Flexible control of downloaded executable content □

Trent Jaeger, Atul Prakash, Jochen Liedtke, Nayeem Islam

May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 2

Publisher: ACM Press

Full text available: pdf(297.79 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a security architecture that enables system and application a ccess control requirements to be enforced on applications composed from downloaded executable content. Downloaded executable content consists of messages downloaded from remote hosts that contain executables that run, upon receipt, on the downloading principal's machine. Unless restricted, this content can perform malicious actions, including accessing its downloading principal's private data and sending messages on th ...

Keywords: access control models, authentication, autorization machanisms, collaborative systems, role-based access control

5 Specifying Kerberos 5 cross-realm authentication □

I. Cervesato, A. D. Jaggard, A. Scedrov, C. Walstad

January 2005 **Proceedings of the 2005 workshop on Issues in the theory of security**

Publisher: ACM Press

Full text available: pdf(228.62 KB) Additional Information: full citation, abstract, references

Cross-realm authentication is a useful and interesting component of Kerberos aimed at enabling secure access to services astride organizational boundaries. We present a formalization of Kerberos 5 cross-realm authentication in MSR, a specification language based on multiset rewriting. We also adapt the Dolev-Yao intruder model to the cross-realm setting and prove an important property for a critical field in a cross-realm ticket. Finally, we document several failures of authentication and confid ...

6 Ada-Java communication in ADEPT □

Anthony Gargaro

November 1997 **Proceedings of the conference on TRI-Ada '97**

Publisher: ACM Press

Full text available: pdf(2.12 MB) Additional Information: full citation, references, index terms

7 Public-key cryptography and password protocols □

Shai Halevi, Hugo Krawczyk

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Publisher: ACM Press

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

8 Ticket based service access for the mobile user □

Bhrat Patel, Jon Crowcroft

September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, references, citings, index terms

9 A methodology for analyzing the performance of authentication protocols □

Alan Harbitter, Daniel A. Menascé

November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 4

Publisher: ACM Press

Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, index terms

Performance, in terms of user response time and the consumption of processing and communications resources, is an important factor to be considered when designing authentication protocols. The mix of public key and secret key encryption algorithms typically included in these protocols makes it difficult to model performance using conventional analytical methods. In this article, we develop a validated modeling methodology to be used for analyzing authentication protocol features, and we use two ...

Keywords: Authentication, Kerberos, mobile computing, performance modeling, proxy servers, public key cryptography

10 Composable ad-hoc mobile services for universal interaction □

Todd D. Hodes, Randy H. Katz, Edouard Servan-Schreiber, Lawrence Rowe

September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(1.86 MB) Additional Information: full citation, references, citings, index terms

11 The KryptoKnight family of light-weight protocols for authentication and key distribution □

Ray Bird, Inder Gopal, Amir Herzberg, Phil Janson, Shay Kutten, Refik Molva, Moti Yung

February 1995 **IEEE/ACM Transactions on Networking (TON)**, Volume 3 Issue 1

Publisher: IEEE Press

Full text available: pdf(1.64 MB) Additional Information: full citation, references, citings, index terms, review

12 Systems Issues: Rajicon:: remote PC GUI operations via constricted mobile interfaces □
Norman Makoto Su, Yutaka Sakane, Masahiko Tsukamoto, Shojiro Nishio
September 2002 **Proceedings of the 8th annual international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, abstract, references, index terms

As of now, it is not uncommon for one to use multiple computers in separate places such as at home, office or school. A number of applications currently exist to allow a user to easily access and control these computers remotely via a notebook computer or web page. Unfortunately, even with such solutions, it is rather inconvenient, for example, to try accessing your computer while walking downtown or riding a train. On the other hand, considering that cellular phones have been accepted as multi- ...

Keywords: GUI, cellular phone, mobile device, remote access

13 Attacking passwords and bringing down the network: Misbehaving TCP receivers can cause internet-wide congestion collapse □
Rob Sherwood, Bobby Bhattacharjee, Ryan Braud
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(258.05 KB) Additional Information: full citation, abstract, references, index terms

An *optimistic* acknowledgment (opt-ack) is an acknowledgment sent by a misbehaving client for a data segment that it has not received. Whereas previous work has focused on opt-ack as a means to greedily improve end-to-end performance, we study opt-ack exclusively as a denial of service attack. Specifically, an attacker sends optimistic acknowledgments to many victims in parallel, thereby amplifying its effective bandwidth by a factor of 30 million (worst case). Thus, even a relatively mode ...

Keywords: congestion control, distributed denial of service

14 The X window system □
Robert W. Scheifler, Jim Gettys
April 1986 **ACM Transactions on Graphics (TOG)**, Volume 5 Issue 2
Publisher: ACM Press
Full text available: pdf(2.76 MB) Additional Information: full citation, abstract, references, citings, index terms, review

An overview of the X Window System is presented, focusing on the system substrate and the low-level facilities provided to build applications and to manage the desktop. The system provides high-performance, high-level, device-independent graphics. A hierarchy of resizable, overlapping windows allows a wide variety of application and user interfaces to be built easily. Network-transparent access to the display provides an important degree of functional separation, without significantly affec ...

15 Cryptography: Password authenticated key exchange using hidden smooth subgroups □
Craig Gentry, Philip Mackenzie, Zulfikar Ramzan
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(300.13 KB) Additional Information: full citation, abstract, references, index terms

Existing techniques for designing efficient password authenticated key exchange (PAKE) protocols all can be viewed as variations of a small number of fundamental paradigms, and all are based on either the Diffie-Hellman or RSA assumptions. In this paper we propose a new technique for the design of PAKE protocols that does not fall into any of those paradigms, and which is based on a different assumption. In our technique, the server uses the password to construct a multiplicative group with a (h ...

Keywords: authentication, cryptography, key exchange, password

16 Cryptographic tools: The dual receiver cryptosystem and its applications □
Theodore Diament, Homin K. Lee, Angelos D. Keromytis, Moti Yung
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(329.14 KB) Additional Information: full citation, abstract, references, index terms

We put forth the notion of a dual receiver cryptosystem and implement it based on bilinear pairings over certain elliptic curve groups. The cryptosystem is simple and efficient yet powerful, as it solves two problems of practical importance whose solutions have proven to be elusive before:(1) A provably secure "combined" public-key cryptosystem (with a single secret key per user in space-limited environment) where the key is used for both decryption and signing and where encryption can be esc ...

Keywords: digital signature, elliptic curves, key escrow, pairing-based cryptography, public key, puzzles, useful secure computation

17 A security architecture for fault-tolerant systems □
Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

18 Certificate-based authorization policy in a PKI environment □
Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

19 Active Proxy-G: optimizing the query execution process in the grid □
Henrique Andrade, Tahsin Kurc, Alan Sussman, Joel Saltz
November 2002 **Proceedings of the 2002 ACM/IEEE conference on Supercomputing**
Publisher: IEEE Computer Society Press
Full text available: pdf(247.81 KB) Additional Information: full citation, abstract, references, index terms

The Grid environment facilitates collaborative work and allows many users to query and process data over geographically dispersed data repositories. Over the past several years, there has been a growing interest in developing applications that interactively analyze datasets, potentially in a collaborative setting. We describe the Active Proxy-G service that is able to cache query results, use those results for answering new incoming queries, generate subqueries for the parts of a query that cann ...

20 Lower bounds on messages and rounds for network authentication protocols □
Li Gong
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, citings, index terms

The encrypted key exchange (EKE) protocol is augmented so that hosts do not store cleartext passwords. Consequently, adversaries who obtain the one-way encrypted password file may (i) successfully mimic (spoof) the host to the user, and (ii) mount dictionary attacks against the encrypted passwords, but cannot mimic the user to the host. Moreover, the important security properties of EKE are preserved—an active network attacker obtains insufficient information to mount dictionary attac ...

Results 1 - 20 of 167 Result page: **1** 2 3 4 5 6 7 8 9 next